Diane Gilzow
February 10, 2026
CYSE 450: Ethical Hacking and Penetration Testing
Dr. Md Morshed Alam

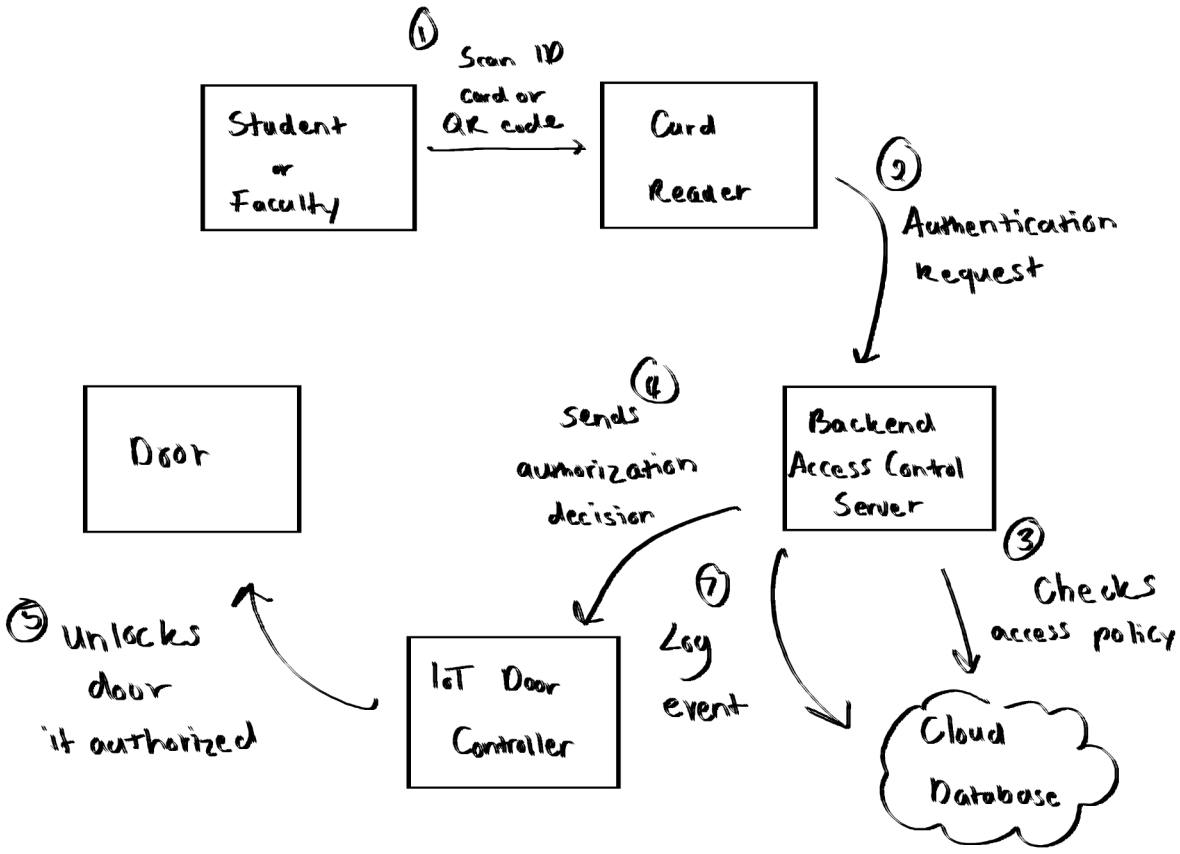
Lab 2: Threat Modeling

- Identify at least 6 critical assets that need to be tested and protected. List them on a table and provide a brief justification of your choice (why it is a critical asset).

Asset	**Justification**
ID Card Data	An ID card can contain personal identifiable information of the holder, such as their name, date of birth, student or faculty information, etc. If compromised, it can be used to gain unauthorized access to restricted areas.
Cloud Database	The cloud database stores access policies and logs that determine who gets access, so it's important that it's protected so that it can't be modified.
Backend Access Control Server	It uses access control to determine who can get access, it needs to be protected to prevent someone from gaining unauthorized access.
Mobile App	The mobile app can also act as an ID card that handles authentication and communicates with the backend server. If compromised, attackers can use it to gain unauthorized access.
IoT Door Controllers (Actuators)	They directly control the physical security of restricted areas, so if they're tampered with, doors could be unlocked without authentication.
Access Logs	Access logs show who has gained access using the card readers. It can show if there has been any unauthorized access, so it's important to keep the logs accurate.

- Draw a Data Flow Diagram depicting the operational flow. Make sure the diagram is hand drawn. You can draw the diagram on a piece of paper and take a snapshot to

attach to your submission.



- Use STRIDE threat model to identify threats per system component. Give a table with the following columns: Component, STRIDE Category, Threat Description.

Component	**STRIDE Category**	**Threat Description**
Card Reader	Spoofing	An attacker can clone an ID card or spoof a QR code to impersonate an authorized user.
Mobile App	Information Disclosure	The mobile app can store sensitive information about the user that can be prone to being exposed.
Backend Access Control Server	Denial of Service	An attacker can flood the server with authentication requests that prevent10

		legitimate users from getting access.
Cloud Database	Tampering	Access policies can be modified to grant access to an unauthorized person, or logs can be deleted to hide malicious activity.
IoT Door Controllers	Spoofing	An attacker can send a forged authorization signal to the controller to unlock the door.

- Using DREAD threat model, rank the identified threats based on risk score. Use Quantitative Risk Assessment as the method to compute the risk score. Use your own metrics and be creative. Make sure the computation process is consistent for all threats.

Threat	**Damage**	**Reproducibility**	**Exploitability**	**Affected Users**	**Discoverability**	**Total Score**	**Risk Probability**	**Rating**
Card Reader Spoofing	10	5	4	1	9	29	58%	Medium
Mobile App Information Disclosure	8	4	4	10	7	33	66%	Medium-High
Backend Server DoS	9	7	8	10	3	37	74%	High
Cloud Database Tampering	10	3	3	4	5	35	70%	High
IoT Door Controller Spoofing	10	3	2	1	8	24	48%	Medium

Threats were rated on a scale of 1 to 10, with 1 being the lowest impact, and 10 being the highest impact.

- Create a defense plan and map each threat with a viable mitigation strategy. Use MITRE ATT&CK Enterprise matrix to determine and refer to the mitigation strategy.

Threat	Mitigation Strategy
Card Reader Spoofing	M1032 - Multi-factor Authentication Use MFA after scanning the ID card or QR code before allowing access. MFA can reduce the risk of an attacker gaining unauthorized access using a fake ID card or QR code. It'll require the user to provide two forms of verification before access can be granted. M1041 - Encrypt Sensitive Information Encrypt communication between card readers and the backend server to prevent interception or replay attacks.
Mobile App Information Disclosure	M1041 - Encrypt Sensitive Information Encrypting sensitive information on the mobile app can reduce the risk of it being disclosed and ensure its confidentiality. Store sensitive credentials, API keys, and configuration files in encrypted vaults. M1057 - Data Loss Prevention Implement DLP controls to monitor and restrict the transmission of mobile app data to prevent unauthorized disclosure.
Backend Server DoS	M1037 - Filter Network Traffic Filter out the attack traffic from the legitimate traffic via protocol-based filtering, enforcing firewall rules, and blocking unknown traffic. M1031 - Network Intrusion Prevention Use intrusion detection signatures to block malicious traffic.
Cloud Database Tampering	M1039 - Environment Variable Permissions Restrict modifications only to authorized users and processes with strict permissions and policies.

	M1041 - Encrypt Sensitive Information Encrypt the database to protect its integrity and confidentiality. M1026 - Privileged Account Management Implement RBAC and least privilege principles to ensure only authorized administrators can modify database policies. This can prevent unauthorized entities from making changes. M1047 - Audit Implement monitoring to detect unauthorized modifications to policies or logs.
IoT Door Controller Spoofing	M1032 - Multi-factor Authentication Require mutual authentication between IoT door controllers and the backend server using certificate-based authentication. This will ensure only trusted devices can communicate with the system. M1041 - Encrypt Sensitive Information Implement encryption for communications between IoT controllers and backend infrastructure. This can prevent attackers from intercepting or modifying access control signals. M1047 - Audit Enable continuous logging and monitoring of door access events, firmware changes, and authentication attempts.